

1 1. In a computer system configured to be capable of receiving presentable
2 content, a method of detecting tampering of the computer system, the method comprising
3 the following:

4 a specific act of booting up the computer system;

5 a specific act of monitoring a signal sequence that occurs internal to the
6 computer system during the specific act of booting up the computer system;

7 a specific act of calculating a boot signature that is a function of the signal
8 sequence;

9 a specific act of comparing the calculated boot signature to an expected boot
10 signature that represents no tampering to the computer system; and

11 a specific act of determining that tampering has not occurred if the
12 calculated boot signature is the same as the expected boot signature.

13
14 2. A method in accordance with Claim 1, wherein the computer system
15 includes a processing device and a memory device, the specific act of monitoring a signal
16 sequence that occurs internal to the computer system during the specific act of booting up
17 the computer system comprising the following:

18 a specific act of monitoring a signal sequence that occurs on a bus
19 connecting the processing device to the memory device during the specific act of
20 booting up the computer system.

21
22 3. A method in accordance with Claim 1, further comprising the following:

23 a specific act of enabling presentable content to be presented if it is
24 determined that tampering has not occurred.

1
2 4. A method in accordance with Claim 3, wherein the presentable content is
3 encrypted presentable content, wherein the specific act of enabling presentable content to
4 be presented comprises the following:

5 activating a decrypter that receives the encrypted presentable content .
6

7 5. A method in accordance with Claim 4, wherein the specific act of
8 monitoring a signal sequence is performed by a boot signature checker circuit that is
9 integrated with the decrypter.
10

11 6. A method in accordance with Claim 4, wherein the specific act of activating
12 a decrypter comprises the following:

13 a specific act of providing the calculated boot signature directly to the
14 decrypter, wherein the decrypter is configured to accept the expected boot signature
15 as a key string needed to activate the decrypter.
16

17 7. A method in accordance with Claim 4, wherein the specific act of activating
18 a decrypter comprises the following:

19 a specific act of providing the calculated boot signature to the decrypter;
20 and

21 a specific act of the decrypter obtaining a key string needed to be activated
22 if the calculated boot signature matched the expected boot signature.
23
24

1 8. A method in accordance with Claim 7, wherein the specific act of the
2 decrypter obtain a key string comprises the following:

3 a specific act of the decrypter obtaining the key string from the memory
4 device.

5
6 9. A method in accordance with Claim 1, further comprising the following:

7 a specific act of determining that tampering has occurred if the calculated
8 boot signature is different than the expected boot signature.

9
10 10. A method in accordance with Claim 9, further comprising the following:

11 a specific act of blocking the presentation of the presentable content if it is
12 determined that tampering has occurred.

13
14 11. A method in accordance with Claim 10, wherein the specific act of blocking
15 the presentation of the presentable content comprises the following:

16 a specific act of deactivating an decrypter that receives the presentable
17 content.

18
19 12. A method in accordance with Claim 10, wherein the specific act of blocking
20 the presentation of the presentable content comprises the following:

21 a specific act of disabling a demodulator such that the demodulator does not
22 demodulate the presentable content.

1 13. A method in accordance with Claim 10, wherein the specific act of blocking
2 the presentation of the presentable content comprises the following:

3 a specific act of disabling a tuner such that the tuner does not tune to the
4 presentable content.

5
6 14. A method in accordance with Claim 10, wherein the specific act of blocking
7 the presentation of the presentable content comprises the following:

8 disabling a central processing unit clock.

9
10 15. A method in accordance with Claim 10, wherein the specific act of blocking
11 the presentation of the presentable content comprises the following:

12 disabling a demultiplexor such that audio, video or other data cannot be
13 extracted from the presentable content.

14
15 16. A method in accordance with Claim 10, wherein the specific act of blocking
16 the presentation of the presentable content comprises the following:

17 disabling a network interface device used by the computer system to
18 interface with a network.

19
20 17. A method in accordance with Claim 1, wherein the specific act of
21 calculating a boot signature that is a function of the signal sequence comprises the
22 following:

23 calculating the boot signature by applying a polynomial expression to the
24 signal sequence.

WORKMAN, NYDEGGER & SEELEY

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

1000 EAGLE GATE TOWER

60 EAST SOUTH TEMPLE

SALT LAKE CITY, UTAH 84111

TOP OF PAGE 2459460

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

1 18. In a computer system configured to be capable of capable of receiving
2 presentable, a method of detecting tampering of the computer system, the method
3 comprising the following:

- 4 a specific act of booting up the computer system;
- 5 a step for calculating a boot signature that is a function of a signal sequence
- 6 experienced internal to the computer system during the specific act of booting; and
- 7 a step for determining whether the calculated boot signature is indicative of
- 8 the computer system being tampered with.
- 9

10 19. A method in accordance with Claim 18, wherein the step for producing a
11 boot signature is performed by a boot signature checker that is coupled to the bus.

12

13 20. A method in accordance with Claim 18, wherein the step for calculating a
14 boot signature comprises the following:

- 15 a specific act of monitoring the signal sequence during the specific act of
- 16 booting up the computer system; and
- 17 a specific act of calculating the boot signature as a function of the signal
- 18 sequence monitored during the specific act of monitoring.
- 19

20 21. A method in accordance with Claim 20, wherein the computer system
21 includes a processing device and a memory device, the specific act of monitoring the
22 signal sequence comprising the following:

23

24

1 a specific act of a boot signature checker monitoring a local bus between the
2 processing device and the memory device to determine a signal sequence that
3 occurs on the local bus during the specific act of booting up the computer system.
4

5 22. A method in accordance with Claim 18, further comprising:

6 a step for acting on the determination of whether the calculated boot signature is
7 indicative of the computer system being tampered with.
8

9 23. A method in accordance with Claim 22, wherein the step for acting on the
10 determination comprises the following:

11 a specific act of activating a decrypter so as to enable the decrypter to
12 decrypt the presentable content.
13

14 24. A method in accordance with Claim 23, wherein the specific act of
15 activating a decrypter comprises the following:

16 a specific act of providing the calculated boot signature directly to the
17 decrypter, wherein the decrypter is configured to accept an expected boot signature
18 as a key string needed to activate the decrypter.
19
20
21
22
23
24

1 25. A computer system capable of receiving presentable content, wherein the
2 computer system comprises:

- 3 a processing device;
- 4 a memory device;
- 5 a bus coupled to the processing device and the memory device;
- 6 a decrypter configured to decrypt encrypted content when activated;
- 7 a boot signature checker that is coupled to the bus so as to be able to read a
8 signal sequence asserted on the local bus during booting of the receiver,
- 9 wherein the boot signature checker is configured to calculate a boot
10 signature that is a function of the signal sequence.

11

12 26. A computer system in accordance with Claim 25, wherein the boot
13 signature checker is directly coupled to the bus.

14

15 27. A computer system in accordance with Claim 25, wherein the boot
16 signature checker is coupled to the decrypter so as to provide the boot signature to the
17 decrypter.

18

19 28. A computer system in accordance with Claim 25, wherein the boot
20 signature checker and the decrypter are integrated within a single physical device.

21

22

23

24

1 29. A computer system capable of decrypting encrypted content, wherein the
2 receiver comprises:

3 a processing device;
4 a memory device;
5 a bus coupled to the processing device and the memory device;
6 a decrypter configured to decrypt encrypted content when activated; and
7 means for calculating a boot signature that is a function of the signal
8 sequence experienced internal to the computer system during booting up of the
9 computer system.
10

11 30. A computer system in accordance with Claim 29, wherein the means for
12 calculating a boot signature comprises the following:

13 a processing device;
14 a memory device;
15 a bus coupled to the processing device and to the memory device; and
16 a boot signature checker that is coupled to the bus so as to be able to
17 monitor the bus for signal sequences.
18

19 31. A computer system in accordance with Claim 30, further comprising the
20 following:

21 a decrypter; and
22 a dedicated connection connecting the boot signature checker with the
23 decrypter.
24

1 32. A conditional access device in accordance with Claim 30, wherein the boot
2 signature checker, the dedicated connection, and the decrypter are integrated within a
3 single physical device.
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24